

The Approach of the Criminal Policy on Eavesdropping and Abusing Internet Data

¹Adel Sarikhani and ²Seyed Mohammed Mousavi

¹Department of Law, University of Ghom, Ghom, Iran

²Azad University of Naragh Branch, Arak, Iran

Abstract: At the present, people are exposed to lose data in different stages of their lives. The outcome of this huge data losing process in people's lives is obtaining the extensive information about other individuals. This information have been found and then recorded, registered in different stages of human's lives. For instance the information related to phone dialogues and finding internet data are of this case. Since, the governments are the encouragers and supporters of using internet, therefore the lawmakers have arranged some good policies due to recording the information.

Key words: Eavesdropping • Data • Internet

INTRODUCTION

The increasing improvement in technology has enabled the usual peoples and governmental offices to listen to the call dialogues and radio signals of people. Telephone, mobile and cells which use the same signals are listenable [1] and the dialogue which are talked on telephones can be coded with a high cost. Besides, decoding the international radio signals, either earth channel or satellite is easy nowadays [2]. For the reasons mentioned above, the privacy of people has been threatened much more than before which cause and bring anxiety and stress. Therefore, governments are trying to support the private territory of people by applying legal techniques and tactics.

Eavesdropping of Phone Calls: In international era, "the international union of overseas communications" is in charge of the arrangement, standardization, confirmation and compatibility and also the development of telecommunication and organizing the policies of overseas communication [3].

In article 37 of statute of this organization on the privacy of the personal communication we have the following states:

- All the members of union have reached to the agreement that they must try their bests to insure the privacy of the international calls of the union.

- Although, the union members have the right of sending these kinds of information to the authorities to apply the national or international rules on them.

Although being top secret of these communications has been strongly emphasized, but there has not been any guarantee for its performance. In Article 34 of the statute, because of the security reasons or other reasons, countries have the right of cutting the personal communications. In statute republic of Iran, we are witnessed of the attention of the lawmaker to this important issue. In criminal judiciary law, the law of establishment of company of communication of Iran (in 1971) has been predicted.

The article 582, Islamic Penalties Law, states that apart from the fact that disgracing people is a criminal action; it expresses penalties on eavesdropping and recording telecommunication and disclosing the information by the authorities and the governmental employees [4].

In Article 582, being governmental employee or a police is the condition of the crime. Consequently, in order to find the cases that are done by other people we need to survey it in other laws.

It is notable that there has not been done any criminology regarding the recording or listening to private phones in other laws. So, according to the comment 7/3472 in 1377/8/16, of judiciary recording or listening to

private telephone calls of others by a government employee is a crime and it is in accordance with article 582 of Islamic Penalties.

But if the third person who is not the governmental officer does this, the criminal investigation is not needed. But if the action is meddling others and call abusing, can be taken to be a criminal act. The phone interference is the issue of the article 641: "If anybody interrupts others by telephone or any other communicational tool, besides the application of the rules of the communicational company, he/she must be imprisoned from 1 month to 6 months [5]. Before the ratification of establishment of communication company of Iran in 1350 and its amendment in 1366 and also the above mentioned article, punishments of all kind of meddling such as letter or call was expressed on articles of moral bylaw.

In 1366 by revising the law of establishment of communication company of Iran, note 2, Article 14, they have considered telephone meddling which is indispensable in Article 641 of Islamic Penalties.

It mentions that, if anybody does meddling with his/her mobile for the first time, his phone will be cut off for one week. and If he/she does the meddling for the second time, his/her mobile will be cut off for 3 months and then the warning letter will be sent to her/his company and If the meddler keep interfering, his phone will be cut off and his deposit will be taken after he pays off all the bills and moneys that he owes. However, the crime mentioned in article 641 is applicable in the case in which the meddling has happened as the result exactly. The interference is a general term, which must be evaluated with the estimation of the action, the character, the tool (Fax, Mobile and others) and so on [6].

The material element of this crime is any kind of communication which leads to the interference or meddling, the repetitive calls which are seen as interferences. For example calling somebody and insulting him or making him sad by bad words are of this case. The spiritual element of the crime are ill will and bad intention beside having the knowledge of this using of the tool, which all these are general ill will and his intend to do the crime in the special ill will of the committer. The important issue is that, according to article 727 claiming to the crime and pursuit of the penalty does not require to the objection of special complainer and also forgiveness of complainer will not stop the pursuit of the committer. The judiciary office, on the comment no. 7/9168, in 08.24.1380, regarding the telephone meddling, not introducing the meddler by the communication company

has been considered as a crime and the communication company must inevitably introduce the meddler. Apart from this, regarding interference in radio signals of others in 1345 has been approved by the parliament and the abuser must be punished. In clause 7, article 11 of this law has been written "If somebody had received a radio message of the people and has used it, is sentenced to 200 Rial to 20,000 Rial in cash. For the fulfilling of the crime in this case, it is necessary that the committer both receive the radio message and also use it. Thus if he has just received the radio message he will not be treated by the above mentioned law. Therefore, receiving only the radio message can't be considered of the crime as a material element.

Detecting and Abusing the Internet Data and Communications: Computers are used comprehensively to create, save and preserve and also send different kinds of information among all people because of its benefits and facilities. These benefits have encouraged people to use computers and internet all over the world in spite of its dangers. Of course the internet has a lot of benefits nowadays; however it cannot put aside the dangers completely.

The extension, facilitation and of course the reduction of the cost in using the computer services of the computer and Internet to have communication is widespread. It is impossible to ask people to work in traditional way since they do their entire educational, official paper, correspondence, bank affairs by Internet; Although Internet has its own shortcoming and dangers. For instance using "Black Box" is the channels of Internet (ISP) for the purpose of supervision the users have been increasingly grown up. Most of the people are not aware of using this technology and based on the little information which is published in this field, most of the systems have "Packet Sniffers" which is used for the security and information purposes by the user of computer channel. These Packet Sniffers are able to supervise all the data streams, the sentences or like the address of the channel or emails. Therefore the black box can record or read the information. Sometimes these systems are at the service of the governmental spy agencies [7].

In spite of the fast improves of the technology, security of the private territory of the internet users is strongly threatened by the abusers. In fact they are moving faster than the technology in improvement. Therefore, the arrangement of the law and the regulations

look necessary and significant for internet services and determining penalties for the abusers seems mandatory. In the legal system of Iran there have not been any laws regarding the internet activities before 2000, but in this year some rules and orders have been ratified and confirmed in this issue. The ratification includes 3 bylaws: The bylaw of getting the permission and the technical regulation of international contacts service, the bylaw of presenting units of informative services and ISP and also the bylaw of services of Internet in café nat. In this bylaws they have mostly focused on how facilitate the condition for the government to have access to internet users activities and information rather than the privacy of their territory.

According to Iran's rules the procedure of getting permission and regulation for international contacts services has been just given for governmental section and the investment by the executive organizations must be under its supervision. According to the article 6 of this bylaw all the telecommunication of Iran has bound to provide all the technical facilities due to the factorization of the system for controlling the channels to preventing users from abusing. The bank of international internet activities must provide the ministry of post and telephones by the users' activities to control and punish the abusers. According to this article there is no specified time limit for keeping this information, in the sense that, this time according to the bylaw is unlimited.

Therefore, the capability of the information bank of the users can be used in different issues for advertising and economical activities and also for discovering and pursuing criminals. In the last paragraph of this article, the other responsibility of the centers of the international contacts points is providing technical facilities to prevent proxy server.

The internet service provider is called ISP. ISP is providing the facilities of internet for people to use internet. ISP is bound to pass all the information which is related to protecting private territory and personal information of the users to them. These units also are banned from any kind of effort to consider or listen to any kind of information box which is sent and received by user. This article completely has been specified in relation with private territory of communication, however each ISP are bound to claim all the general information of the users and their IPs related to their registration and report and version to the post and telephones minister. The same regulation has been come in bylaw of the café net.

In the article of the bylaws, ISP is expressed as a guarantee for execution of the regulation. According to this, regarding violation, the imposed penalties include warning, reprimand, canceling the sanction and sending to court which are based on the type of the crime. The total of the regulations, basically is expressive of all the information of users is available by the governmental authorities. This bank of information has been saved beside ISP for unlimited time. According to this, it's suggested that the creators of ASP & ISP should save all the internet communication of their own users for 6 months. But access to the internet communication is only legalized by the permission of judicial Authorities. Although after this period if the judicial Authorities don't want the organization to save somebody's data for a longer time it must delete all the information. If anybody violate, he must be punished. In the penalties of the Islamic law, the guarantee and arrangement of performance has been approved in field of computer including 55 articles in 1388 [8]. The following articles are of this case.

Article 762 acknowledges that, "Whenever the record of a saved computer data comes to be necessary for the judicial authorities they can give the right of keeping and saving the information to one under their control. In the case of the emergency, like having danger of getting damaged or changed or losing the data, they can order to protect and the process must be passed to judicial authority in 24 hours. If one of the staff or judicial positions disclose the data or inform the one whose data is controlled about the order or abuse the data he must be punished from 91 days to 6 months imprisonment or must be charged from 5 million Rial up to 10 million Rial in cash or both of them.

Note 1: The data saving means to protect them as orders not to disclose or abuse them.

Note 2: The time of keeping the information is maximum 3 months and it is extendable by the order of judicial position [9].

CONCLUSION

Along with the progress of technology in different fields such as information and communication, privacy of people has been confronted with dangers and threats in comparison with the past. Using the instruments such a computer and internet is the possibility of facilitation in

communication and collecting information. But this kind of technology is the best way to penetrate to the privacy of the users by the government or any other individual. This problem brought a big concern throughout the world, thus the international society and the lawmakers want to find a preventive way of this issue and they want to find a way of getting rid of this problem.

Besides the technology progress is field of information and communication, a lot of dangers and problems have been brought up and the security and privacy of the people has been threaten. Microphones and cameras and also some satellite uses are of this case. And all has affected the security of the people and they have both advantages and disadvantages. Therefore, some professional and proficient laws must be predicted in the sense of international affairs in the issue and the protection of the privacy of people and their information must be guaranteed and the security abusing must be vanished.

REFERENCES

1. Pad, E., 2006. The special criminal laws. Vol 1. Daneshvar publisher, Tehran.
2. Ansari, B., 2007. The laws of private territory, Samt Publisher, pp: 289.
3. Anonymous, 2011. International telecommunication on union at: // WWW. Itu. Int/home.
4. Sarikhani, A., 1999. Spying and being against the country. Tablighat office publisher, Ghom.
5. Goldoozian, E., 2003. On the Islamic criminal policy laws, Majd Publisher, 5th edition.
6. Aghaeenia, H., 2007. Crimes against the individuals, Nashre Mizan Publisher, Tehran, second edition.
7. Anonymous, 2003. Pnvacy and Human Rights. Theras to Privacy: available at: // WWW. Drivacyin ternational.com.
8. Anonymous, 2009. The laws of the computer crimes. Articles: 729 to 782 and also Articles, pp: 784-785.
9. Jahangiri, M., 2011. The Islamic Criminal Laws, Didar Publisher, Tehran.